qrulepubliccomments

From: Linda Ackerman [lga@privacyactivism.org]
Sent: Monday, January 30, 2006 3:14 PM
To: qrulepubliccomments
Subject: Comments: RIN 0920-AA03

Attachments: CDC.Comments.Final.060130.doc

CDC.Comments.Final.060130.doc ...

Attached as MS Word file.

January 30, 2006

Centers for Disease Control and Prevention
Division of Global Migration and Quarantine
1600 Clifton Road, NE., (E03)
Atlanta, GA 30333

Filed electronically at: http://www.regs.gov

Re: Notice of Proposed Rulemaking
Department of Health and Human Services
42 CFR Parts 70 & 71
RIN 0920-AA03
Control of Communicable Diseases

These comments are submitted by Privacy Activism, Privacy Rights Clearinghouse, Fairfax County Privacy Council

Privacy Activism is a California nonprofit educational organization that works on behalf of consumer privacy issues. Our particular area of interest is information privacy and the collection and use of personal information in government and commercial databases. www.privacyactivism.org

The Privacy Rights Clearinghouse is a nonprofit consumer education and advocacy organization based in San Diego, CA, and established in 1992. The PRC advises consumers on a variety of informational privacy issues, including financial privacy, medical privacy and identity theft, through a series of fact sheets as well as individual counseling available via telephone and e-mail. It represents consumers' interests in legislative and regulatory proceedings on the state and federal levels. www.privacyrights.org

FCPC was established in 2003 to focus attention on privacy issues affecting Virginians. FCPC is a member of the Liberty Coalition and the Coalition for Constitutional Liberties, but we are not registered with any government agency because we do not need the government's permission to speak freely and assemble ideas. www.FairfaxCountyPrivacyCouncil.org

CONTENTS

1. Introduction……2
2. Scope of Proposed Regulations……..2
3. A Cautionary Tale……...3
4. Legal Authority……...……8
5. Administrative Search and Seizure…….8
6. Due Process and Quarantine……..14

7. Passenger Data……..17
8. Mission Creep……23
9. Conclusions……24
Appendix A……..…25

1 Introduction

The Centers for Disease Control and Prevention (CDC) proposes to protect the public health against the spread of specific natural and bioengineered communicable diseases by creating a two-part system that will apply to all air and ship passengers, both international travelers to the United States and domestic travelers between and within the states. The system consists of 1) passenger inspection, quarantine and reporting; and 2) a database of personal information for the purpose of contacting dispersed passengers who may be at risk of infection.

The commenters recognize the significant public health need that the CDC's proposed regulations address. It is important to take reasonable steps to prepare against the likelihood of a serious communicable disease spreading to become a pandemic. Prior planning and organization are necessary in order to contain such a disease, to minimize the death toll, and modulate the impact such an episode could have on global social, economic and political stability.

We have concerns, however, about many aspects of the proposed information collection and security processes. We also question what we believe are vague criteria and screening procedures involved in determining who is an "ill person"; these questions in turn raise Fourth and Fourteenth Amendment issues about the screening process. And we believe that the absence of due process in the case of provisional quarantine raises constitutional concerns, and that the regulations for appealing full quarantine are confusing. Finally, we take issue with the application of the proposed regulations to interstate travel, which we believe raises constitutional issues under the First Amendment, as well as the Fourth and Fourteenth Amendments.

2 Scope of the Proposed Regulations

Two generally overlapping sets of regulations are proposed. The first is 42 CFR Sec. 70, which is intended to "prevent the introduction, transmission, and spread of communicable diseases from one State into any other State." The second set of regulations, 42 CFR Sec. 71, applies to the "introduction, transmission, and spread of communicable diseases from foreign countries into the United States' and to "prevent[ing] the spread of disease among possessions of the United States or from a possession into a State."

The regulations discussed in these comments are principally the following:

- Parts 70.1 and 71.1: scope and definitions
- Parts 70.4 and 71.10: passenger information, dealing with who shall collect the information, what information shall be collected, limits to the use of the information and notice to passengers of the purpose for information collection
- Parts 70.13 and 71.16: screenings to detect ill persons, concerning the criteria and methods by which initial judgment of illness shall be made.
- Parts 70.14 to 70.18 and 71.19 to 71.21: provisional quarantine, quarantine, quarantine orders and service.
- Parts 70.19 and 71.22: medical examination and monitoring
- Parts 70.20, 17.23, 17.31: hearings

3 A Cautionary Tale

The history of the Transportation Security Administration's (TSA) efforts to develop an airline passenger screening system should be taken by the CDC as a caveat of mistakes not to repeat in developing its own passenger-contact database and in handling personal information. The TSA has now been at work for at least four years on a system originally called CAPPS II (Computer Assisted Passenger Prescreening System) and now called Secure Flight. For about the first 11 months of the program, from February 2002 to January 2003, the agency or its contractors tested passenger records it requested from most major U.S. airlines with no notice to the public. As of January 2006, after spending [$?], the TSA still does not have an operative system. Instead it has a tarnished reputation and has earned the distrust of the public, the airlines, and other government agencies.

CDC faces at least two of the same problems that TSA has not been able to overcome. One is public wariness about the government's use of personal information, regardless of the stated purpose. Even with transparent intentions and conscientiously secure information handling practices, there will be skepticism about why the CDC needs so much personal information to accomplish its goals and what other government agencies will have access to the data and why. The other is that there is an enormous technical gap between saying that airlines and cruise lines must modify their current reservation databases and storage practices to accommodate the CDC's data requirements, and must transfer data to the CDC on demand, which the CDC will be able to read and use, and actually achieving that goal. TSA's system requirements are more complex, but the fact remains that it has yet to develop a viable system for using passenger records for security purposes, or even to figure out what information it needs to achieve its goals.

The Department of Transportation (DOT) first publicly proposed creating a system of airline passenger records, enhanced by commercial data that included financial and credit card records, in January 2003 (see Federal Register: January

15, 2003,Volume 68, Number 10, DOCID:fr15ja03-20). An outpouring of negative comments forced the TSA, which had taken over the project and moved to the Department of Homeland Security (DHS), to publish revised rules in July 2003 (http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket. access. gpo.gov/2003/pdf/03-19574.pdf), which generated further negative comments.

Meanwhile, in February 2003, TSA announced that it would begin testing CAPPS II. When news broke in March that Delta would be the test airline and the general public became aware of TSA's plans, there was considerable negative publicity and a campaign was mounted to boycott Delta. ("Privacy Activist Takes on Delta," Wired News, March 5, 2003, http://www.wired.com/news/privacy/ 0,1848,57909,00.html; "Travel Industry and Privacy Groups Object to Screening Plan for Airline Passengers, New York Times, March 6, 2003http://www.nytimes. com/2003/03/06/business/06FLY.html) Objections to CAPPS II continued in Congress and the media until DHS Secretary Ridge announced that testing would not begin until the department hired a Chief Privacy Officer to review the passenger screening plan. ("Homeland privacy officer to review passenger-screening system," National Journal's Technology Daily, April 9, 2003, http://www.govexec.com/dailyfed/0403/040903td1.htm) In June 2003, CAPPS II testing was supposedly suspended ("CAPPS II Testing on Back Burner," Wired News, June 13, 2003,http://www.wired.com/news/privacy/0,1848,59252,00.html); in August DHS again said it intended to implement the program ("DHS stands behind CAPPS II," Federal Computer Week, August 26, 2003, http://www.fcw. com/fcw/articles/2003/0825/web-capp-08-26-03.asp).

In September 2003, Congress ordered that CAPPS II not be deployed "until the General Accounting Office certifies . . . that the system will not finger too many innocent passengers" ("Congress Puts Brakes on CAPPS II," Wired News, September 26, 2003, http://www.wired.com/news/politics/ 0,1283,60600,00.html). Shortly before, jetBlue had announced that it would provide passenger records for CAPPS II testing ("jetBlue Data to Fuel CAPPS Test," Wired News, September 16, 2003, http://www.wired.com/news/ privacy/0,1848,60456,00.html); later, it was revealed that starting in the spring of 2002 the airline had turned over 5 million passenger records, in violation of its own privacy policy, with no Privacy Act notice from TSA, at least nine months before its first CAPPS II Federal Register notice in January 2003.

This, however, was the barest tip of the iceberg. In June 2004, after months of denials by TSA to the public, Congress, the Government Accountability Office (the renamed General Accounting Office), and the DHS Chief Privacy Officer, David Stone revealed in answers to a questionnaire from the Senate Governmental Affairs Committee considering his nomination to be an assistant secretary of DHS for TSA, that as far back as February 2002 TSA had been receiving passenger records from the airlines. Cooperating companies included American, Delta, United, Northwest, America West, jetBlue and Frontier, along with the Galileo International and Sabre computerized reservation services

(CRSs) Passenger information was turned over directly to private contractors, some working for the Defense Department (Torch Concepts) and others for TSA (HNC, Infoglide, IBM, Ascent, Lockheed, Acxiom) (see http://www.epic.org/privacy/airtravel/stone_answers.pdf, pages 15-19). These rather tawdry revelations led to many individual and class action lawsuits, first against jetBlue and TSA, then against the private contractors other airlines involved. Airlines consequently refused to transfer more passenger data to TSA; the agency in turn announced that it would compel them to ("U.S. to force airlines to provide traveler data," Reuters, March 17, 2004, http://www.reuters.com/newsArticle.jhtml;jsessionid=H0B5RYG1ZLRJCCRBAELCFFA?type=topNews&storyID=4591707).

In February 2004, the GAO issued the report Congress had requested in September 2003. It concluded that TSA had failed to address seven of eight major issues concerning CAPPS II, including setting out policies for operation and use of the system, privacy and redress (http://www.gao.gov/new.items/d04385.pdf). The DHS Chief Privacy Officer's report on the jetBlue transfer followed shortly. It found that TSA's requesting passenger records from the airline and turning them over to a defense contractor "raises serious concerns about the proper handling of personally identifiable information by government employees within the Department of Homeland Security," (see "Report to the Public on Events Surrounding the jetBlue Data Transfer," http://www.epic.org/privacy/airtravel/jetblue/dhs_report.pdf, p. 1) After more Congressional hearings, more lawsuits, more policy changes—including the appointment of a TSA Privacy Officer—and regular delays in planned implementation of CAPPS II, Secretary Ridge announced in July 2004 that CAPPS II was being scrapped. In August 2004, it re-emerged as "Secure Flight" ("TSA unveils new passenger prescreening program," Government Computer News, August 26, 2004, http://gcn.com/vol1_no1/daily-updates/27077-1.html).

TSA kicked off Secure Flight by ordering airlines to turn over all passenger records from June 2004 for testing (see Transportation Security Administration, [Docket No. **TSA**-2004-19160], Privacy Impact Assessment—the notice ordered airlines to transfer the requested records by November 23, 2004, Secure Flight Test Phase; "Fliers face new scrutiny, but this time with a twist," USA Today, September 27, 2004, http://www.usatoday.com/news/opinion/editorials/2004-09-27-our-view_x.htm). TSA received more than 500 public comments on its PIA; changing the name of the program did not end the controversy about commandeering passenger records and the personal information they contained, or about the TSA's constantly shifting explanations of what it proposed to do with the data and how the agency handled it.

Before TSA could deploy Secure Flight, however, it needed GAO's approval that it had addressed the deficiencies noted in GAO's February 2004 report; i.e., that it had a plan and a budget (see "Air-Travel Screening Snagged," Washington Post, November 20, 2004, http://www.washingtonpost.com/wp-dyn/articles/A63951-

2004Nov19.html). GAO gave what can barely be described as consent in its March 2005 report, "Secure Flight Testing Under Way, but Risks Should Be Managed as System Is Further Developed (http://www.gao.gov/new.items/d05356.pdf). It noted that TSA had not yet finalized its system requirements or operating policies and that although it had developed tests for matching passenger data against security watch lists, it had not yet completed testing. In March 2005, TSA announced that it expected to roll out Secure Flight with two unidentified airlines in August ("TSA, 2 Airlines To Test Secure Flight," Business Travel News, March 21, 2005, http://www.btnmag.com/businesstravelnews/headlines/frontpage_display.jsp?vnu_content_id=1000846203).

In April 2004, DHS Chief Privacy Officer Nuala O'Connor Kelly appointed a committee to advise the department how best to protect citizen privacy in the post-9/11 security environment. Among the first things privacy advocates asked the panel to do was evaluate Secure Flight (Panel Urged to Review Passenger Screening; Security System Raises Privacy Concerns, Washington Post, April 7, 2005, http://www.washingtonpost.com/wp-dyn/articles/A32842-2005Apr6.html). Meanwhile, the TSA's Privacy Officer had appointed a committee, the Secure Flight Working Group (SFWG) in January 2005 to evaluate the privacy and security aspects of Secure Flight.[1] The SFWG initially was given information on Secure Flight test results, probable data needs, plans for information transfer, and redress but received no new information after March. In September 2005, the SFWG submitted a report to TSA stating that it could not evaluate Secure Flight's privacy and security components because it had insufficient information to do so. The group concurred with the March 2005 GAO report that TSA had yet to fully define an operational plan for Secure Flight ("Report of the Secure Flight Working Group, Presented to the Transportation Security Administration, September 19, 2005, http://www.epic.org/privacy/airtravel/sfwg_report_091905.pdf; see also "Report: U.S. Needs to Get Screening Right,"AP via The Washington Post, September 23, 2005,http://www.washingtonpost.com/wpdyn/content/article/2005/09/23/AR2005092301737.html).

In May 2005, the House Appropriations Committee cut $15 million from Secure Flight's requested budget, stating that too many critical issues concerning the program remained unresolved ("Airline screening program panned by House appropriators, GovExec.com, May 11, 2005, http://www.govexec.com/dailyfed/0505/051105cdpm3.htm). In June it was revealed that TSA and its contractor EagleForce had acted beyond the scope of the September 2004 Secure Flight PIA by using commercial data in its tests. The company had generated more than 200,000 variations of names from the 40,000 passenger records actually used, thus invading the privacy of many people who did not fly in June 2004 and therefore had no notice of the government's use of their personal information and had stored the information insecurely on CDs. In other words, TSA had generated more names from the 40,000 June 2004 passenger records it had decided were useful and its contractor had augmented the resulting list of around 250,000

[1] Linda Ackerman, of Privacy Activism, was a member of the Secure Flight Working Group.

names with commercial data. The DHS Chief Privacy Officer said she would begin an investigation of TSA's information handling practices ("TSA Illegally Collects Personal Data on Airline Passengers," AP via Capitol Hill Blue, June 21, 2005, http://www.capitolhillblue.com/artman/publish/article_6902.shtml). In July, the GAO wrote a letter to Congress that TSA had violated the Privacy Act (GAO Letter to Congress, July 22, 2005, http://www.gao.gov/new.items/d05864r.pdf). On June 22, 2005, TSA published a Federal Register notice stating it would do the things it had already done that were in violation of its previous notice (Transportation Security Administration, [Docket No. TSA-2004-19160], "Privacy Act of 1974; Systems of Records: Secure Flight Test Records; Privacy Impact Assessment; Secure Flight Test Phase").

Undeterred, Secure Flight director Justin Oberman announced in August 2005 that more unnamed airlines would participate in the screening system's roll-out in September (later pushed back to October, and then to "early 2006") ("U.S. Air Screening May Be Expanded Beyond 2 Carriers," Bloomberg, July 26, 2005, http://www.bloomberg.com/apps/news?pid=10000103&sid=aVcyDx9HUGU8&refer=us). In September, TSA was strongly criticized in a redacted report prepared by the Justice Department's Office of the Inspector General at the request of Congress. The report stated that the FBI's Terrorist Screening Center (TSC) could not support TSA's passenger screening program because TSA had failed to "make, communicate and comply with key program and policy decisions in a timely manner, such as the launch date [of Secure Flight] and volume of screening to be conducted during the initial implementation phases." ("Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program," p. iii, http://www.usdoj.gov/oig/reports/FBI/a0534/final.pdf) This was a polite way of saying what others had already said repeatedly: TSA did not have an articulable program or policies for a passenger screening system.

Work on Secure Flight continues, but at least publicly TSA seems to be focusing more on other aspects of its "multi-faceted" airline security program. It has announced that it is expanding pilot programs for registered traveler programs, which are less controversial because participants voluntarily give their personal information (http://www.tsa.gov/public/display?theme=8&content=9000519800b4ddd). It is also recently began combining a "risk-based assessment" of passengers by airport screeners, leading to secondary physical screenings, with permission to bring some sharp objects on board ("New Airport Screening Policies In Place For Holidays," December 21, 2005, http://www.foxreno.com/news/5598522/detail.html; see also The Onion on TSA's new screening guidelines, http://www.theonion.com/content/node/43716).

The point of this lengthy summary is cautionary. CDC should not begin development of its quarantine reporting and passenger contact system without a fully articulated plan that includes system architecture and all operational policies, including those for information privacy and security. That plan may change over

time in response to testing outcomes or unforeseen requirements, but it would be a fatal mistake to set out with only a goal in mind and no clear idea how to reach it. It is not enough to tell carriers and GDSs (global distribution—or reservation—systems) to "make it so." CDC should also execute its plan with minimal intrusion into personal privacy and its information handling practices should demonstrate clearly at every step of the way that it respects the privacy of the traveling public.

4 Legal Authority

We believe that 42 USC §264 (§361) and the Commerce Clause of the U.S. Constitution authorize the CDC to compel carriers and GDSs to collect data that is in addition to what they currently collect when they take passenger reservations and to turn it over to on request. Data collection is necessary to track the extent and location of communicable diseases, both individually and in the aggregate. In particular, the ability to contact people who may be infected, in order to quarantine and treat them, is essential to containing potential epidemics.

We question, however the extension of this authority, and how the CDC proposes to exercise it, into interstate commerce, where we believe the border exemptions and other circumstantially reduced expectations of privacy cited to justify administrative search and seizure should not apply. The CDC's compelling interest is not in doubt, but it appears to claim a great deal of discretion to search and detain (i.e., quarantine) people in interstate travel. These intrusions bring the regulations into conflict with First Amendment freedom of movement and the right to travel, as well as the freedom of association. They also raise Fourth Amendment issues concerning warrantless searches (inspection for illness) and seizures (provisional quarantine and full quarantine). We will set forth our specific questions and objections in the body of these comments.

5 Administrative Search and Seizure

The commenters have two principal concerns with the impact of the proposed regulations on Fourth Amendment search and seizure:

- We believe that the CDC is pushing the limits of warrantless administrative search and seizure, particularly where persons, rather than property, are concerned.
- While we acknowledge that there is a reduced expectation of privacy at international borders, we do not believe that same case law-derived claims can be made for travelers arriving at interstate airport destinations.

Case Law Justification of Administrative Search and Seizure.
The CDC proposes to conduct searches (screenings to detect ill persons) and seizures (provisional and regular quarantines) of arriving airline and ship passengers. The explanations for the regulations involved—Parts 70.13-14, 70.16,

70.19 and Parts 71.16-17, 71.19, 71.22—and the case law offered to support them, note that, especially in the context administrative enforcement, many types of search and seizure done without a warrant and in the absence of probable cause have been upheld by the federal courts.[2] The CDC maintains that the proposed regulations are consistent with the three-part test laid out by the Supreme Court in a case involving a warrantless inspection of an auto junk yard, a closely regulated business (i.e., a business comparable to an airline, because its operation is subject to some amount of government regulation). The court held that such a search required that "(1) there is a substantial government interest that informs the regulatory scheme pursuant to which the inspection is made; (2) the warrantless inspection is necessary to further the regulatory scheme; and (3) the inspection program, in terms of the certainty and regularity of its application, provides an adequate substitute for a warrant." (*New York v. Burger*, 482 US 691, 702-703 (1987)

The CDC cites additional case law in support of a diminished expectation of privacy for people in transit on "common thoroughfares," including planes[3]; at international borders[4]; and for regulated commercial industries generally[5]. The only case cited in support of search and seizure of a *person* at an international border is *U.S. v. Montoya de Hernandez*, 473 US 531, 544 (1985), an alimentary canal drug smuggling case. In *Montoya*, "the Supreme Court analogized holding a suspected alimentary canal smuggler to detaining someone for suspected tuberculosis, noting that 'both are detained until their bodily processes dispel the suspicion that they will introduce a harmful agent into this country.'"[6] We would distinguish *Montoya* because it involves search and seizure based on suspicion of criminal activity.

The CDC also relies on case law for the assertion that "Anyone who possesses common authority over or other sufficient relationship to the premises or effects sought to be inspected may consent to the search of another's property." (*Lenz v. Winburn*, 51 F.3d 1540, 1548 (11th Cir. 1995); concerning removal of personal property in a child custody case) By extending the reasoning in this case to a factual situation that is not even remotely similar, the owner or commanding officer of a plane or ship could presumably consent to a search of the property (such as baggage and cars) of those on board. Even if this decision is followed, its

[2] See pp. 71894-71896.
[3] *US v. McDonald*, 100 F.3d 1320, 1324-25 (7th Cir. 1996) (noting that it's generally recognized that people who are in transit on common thoroughfares, i.e., on a bus, train, or airplane, have a substantially reduced expectation of privacy compared to persons in a fixed dwelling).
[4] *U.S. v. Berisha*, 925 F.2d 791, 795 (5th Cir. 1991) (incoming and outgoing border searches have features in common including the need to protect U.S. citizens, the likelihood of smuggling contraband, and the fact that individuals are placed on notice that their privacy may be invaded when they cross the border). See also *U.S. v. Flores-Montano*, 541 US 149, 152 (2004) (the government's interest in preventing entry of unwanted persons and effects is at its zenith at the international border and border searches are part of the sovereign right of self-protection and logically must occur at the border). The facts of the *Flores* case, though, involve the removal and inspection of a gas tank from a car, not a search and seizure of a person.
[5] *New York v. Burger*, 482 US 691 (1987)
[6] See p. 71896.

fact situation is so unlike "screening for ill persons" there is no reason to assume that it extends to the ability of an airline "authority" to consent to the search of individuals on board.

We believe that all the cases the CDC cites in support of its administrative powers of search and seizure and of circumstantially diminished rights to privacy are distinguishable from search and seizure that involves medical screening and quarantine and also that the standard for search and seizure of persons should be higher than the standards for property: "[T]he threshold consideration is the level of intrusiveness of the search and that, generally, a search of a person will likely invoke intrusiveness considerations different and more significant than those of a search of the person's effects." (*U.S. v. Lawson,* 74 F.Supp.2d 513, 519 (ED Kentucky, 2005)

Accordingly, we offer the standard for administrative searches proposed by U.S. Court of Appeals Judge Alex Kozinski:

> "Administrative searches are an oddity of Fourth Amendment jurisprudence. They involve judicially-approved searches and seizures of countless people and places, with no particularized suspicion and normally without a warrant. To justify such a wholesale exemption from ordinary Fourth Amendment requirements, the government must establish two critical elements: first, that there's a compelling need for the intrusion; and second, that the intrusion is strictly limited to fulfilling that need." (*United States v. $124,570 U.S. Currency (Campbell),* 873 F.2d 1240, 1244-45 (9th Cir.1989). *U.S. v. Soyland,* 3 F.3d 1312, 1316 (9th Cir. 1993)(Kozinski, J. dissenting)

Criteria for What Constitutes a Compelling Need to Search for Signs of Infectious Disease Are Unclear.

Containing the spread of a dangerous communicable disease may be a compelling reason for the CDC to act without individualized suspicion or a warrant—at least at international borders, where its actions are part of the government's sovereign powers to control entry and protect against unlawful (criminals, drugs) or unwanted (disease) admissions. But it is not clear from these regulations what constitutes a compelling public health need, and the definitions (Part 70.1) leave it to the discretion or judgment of the Director of CDC or the Secretary of HHS to decide:

> Public health emergency, as used in this part, means:
> (i) Any disease event as determined by the Director with either documented or significant potential for regional, national, or international disease spread or with actual or potential interference with the free movement of people or goods between States and possessions within the United States or other countries or sovereignties; or

> (ii) Any disease event designated as a public health emergency by the Secretary, pursuant to Sec. 319(a) of the Public Health Service Act (42 USC 247d(a)).

These standards leave a great deal of latitude to take intrusive measures without precisely defining the criteria for doing so. For example, avian flu is currently in the news and there are daily reports of its case-by-case (or fatality-by-fatality) and country-by-country spread. Cases of human infection in the single digits have now been reported in Indonesia, Vietnam, China, Laos (or not; the news has been reported both ways for Laos), Cambodia, Thailand and Turkey. At what point, based on what information do the movement and magnitude of this communicable disease (if it is found to be one) reach critical mass and trigger the proposed inspection and quarantine regulations?

Uncertainty about what amounts to a compelling need calls into question the legitimacy of the broad justification for search and seizure the CDC claims. Such vague standards will undoubtedly produce many false positives that will result in three business days of provisional quarantine, for which there is currently no recourse to appeal or contest (Parts 70.14 and 71.17). There must be a more equitable balance between the CDC's compelling need and rights protected under the First, Fourth and Fourteenth Amendments.

The Scope of the Director of CDC's Authority Is Extremely Broad.
The Federal Register notices states:

> The Director's authority to investigate suspected cases and potential spread of communicable disease among foreign and interstate travelers is thus not limited to those known or suspected of having a quarantinable disease. . . [current list of quarantinable diseases is at http://www.cdc.gov and http://www.archives.gov/federal_register]. Rather, the authority encompasses all communicable diseases that may necessitate a public health response.[7]

One way to read this statement of the CDC Director's authority to interfere with the Fourth Amendment rights of international, and more importantly, interstate travelers, is that nothing more than a generalized idea that someone may have been in an area where a quarantinable disease, or a communicable disease that requires a public health response, is present. On what basis can the Director justify investigating people who are neither "known or suspected of having a quarantinable disease?" This is too broad and vague a justification for medical search and seizure in the form of screening for illness, which could result in a provisional three-day quarantine without access to any form of hearing.

Screening for Ill Persons Is a Search Without Particularized Suspicion.
It is the screening of arriving passengers for signs of illness that generates

[7] Page 71899.

suspicion that they may have an infectious disease in the first place; the search precedes the suspicion. Such a search must be justified under special or compelling need (which we question based on vague criteria of what constitutes a compelling need to trigger passenger screening), generalized administrative search of a regulated industry (a weak argument for searches of persons), or "border" (supported at international borders by case law). What the CDC may be considering, but does not refer to in its Federal Register notice, is substituting ethereal and notionally infallible technology for supposedly more subjective and arguably more intrusive human screeners.

In May 2003, the *New York Times* ran a story titled, "Military Hardware Is Adapted to Fight SARS." Singapore's Ministry of Health asked the country's Defense Science and Technology Agency to develop a more efficient way to screen arriving passengers for high fever than having them walk past a phalanx of nurses. They modified military thermal imaging scanners to measure human skin temperature "to within a half a degree at 15 feet" and display it as a color-coded video image; anything at 99.5 degrees or higher glows bright red. (http://www.nytimes.com/2003/05/12/technology/12SCAN.html?ei=5007&en=215ca159e2e62fa0&ex=1368158400&partner=USERLAND&pagewanted=all&position=; mirrored at http://www.interesting-people.org/archives/interesting-people/200305/msg00130.html; see Appendix A for the full article)

Clean and remote, perhaps, with no direct visual inspection or intrusive thermometer, but not exactly infallible. An operator of the device at Changi Airport observes that "a sunburn, a few drinks of alcohol or some brisk exercise" or eating mutton or smoking a cigarette "might raise skin temperature enough… [to] produce a red response." In other words, even a high-tech search will result in a lot of false positives that will lead to inappropriate provisional quarantines.

Whether initial screening for ill persons is done by human observation or remote skin temperature sensing technology, nothing in the record supports the assertion that these means are effective and narrowly tailored.

Search and Seizure at Interstate Transit Points.
Regarding the CDC's authority to screen for illness and to quarantine interstate travelers at airport transit points, there is a similar compelling interest at stake, although we have the same reservations about the vagueness of criteria for deciding the "what" and "when" issues of imposing screening and quarantine as we have for international borders. We also acknowledge regulatory power under the Commerce Clause. As the Federal Register notice states:

> The proposed regulation is consistent with the scope of the federal government's commerce power because it seeks to regulate the uses of the channels of foreign and interstate commerce (i.e., by protecting against the introduction, transmission, and spread of communicable diseases) and the instrumentalities of foreign and interstate commerce (e.g., airlines with

flights arriving into the U.S. or traveling from one state or possession into another).[8]

Application of the CDC's regulatory power over the instrumentalities of interstate commerce to protect against the spread of communicable diseases, however, comes into serious conflict with rights guaranteed under the First Amendment. That is, the right to travel, freedom of movement, and freedom of association. Even with a compelling interest, these rights require careful balancing and carefully tailored regulations that do not unduly impinge on fundamental freedoms.

We believe that the border exception should not automatically apply to administrative searches of interstate airline passengers. The discretion of the CDC Director to order such searches should be based on a probable cause standard for taking the action, if not on probable cause itself. There must be a reasonable basis to suspect that a quarantinable or communicable disease is actually present before a planeload of domestic passengers can be subjected to screening and provisional quarantine for three days without recourse. Epidemiological data about the area from which a domestic airport draws its passengers, plus similar data about a traveler's city and state of residence should be factors in determining if there is probable cause to screen people.

Screening and Due Process.
The regulations give a great deal of attention to due process in the event of quarantine (though not provisional quarantine), but say nothing about due process as part of the screening process. We believe this is an omission that needs to be addressed. Screening, as defined in Parts 70.13 and 71.16 is broad and vague, to be done by "means determined appropriate by the Director." This could include anything from visual observation to temperature taking by various means, most of them physically intrusive. Also, the definition of "ill-person" (Parts 70.1 and 71.1) has specificity but is ultimately quite open-ended, covering anyone who "Displays symptoms or factors that are suggestive of a communicable disease."

It seems clear that any such screening must be subject to carefully defined criteria and procedures. Very importantly, for example, it is not clear whether the power to conduct screening includes the power to detain in order to screen for illness. Also, who will conduct the screening? Although we are told that the CDC's own "quarantine officers are typically the first line of defense in preventing the importation of communicable diseases into the United States,[9] the sections requiring a designated agent to communicate the presence on board a carrier of an ill person assume that an airline employee will make the determination (see Parts 70.2 and 71.6). In some cases illness will be clear even to an untrained observer; however, as with thermal-imaging technology, a crew member could easily attribute the effects of sunburn or a few drinks to sickness. Someone with no

[8] Page 71894.
[9] Page 71895.

medical training whatsoever is not qualified to determine whether a passenger needs further screening.

6 Due Process and Quarantine

The CDC acknowledges that due process applies to its quarantine regulations. The question, then, is whether the regulations provide as much process as is due under the circumstances. To decide, the CDC applies a balancing test— "balancing the private interest affected by the official action against the government's asserted interest and the burdens that the government would face in providing greater process," as the CDC's Federal Register notice has it, citing *Hamdi v. Rumsfeld*, 542 U.S. 507, 529, 124 S.Ct. 2633, 2646 (2004).[10] However, the CDC's equation is incorrect, because it does not quote fully from *Mathews v. Eldridge*, 424 US 319, 335 (1976), on which Hamdi relies: "T he process due in any given instance is determined by weighing 'the private interest that will be affected by the official action' against the Government's asserted interest, 'including the function involved' and the burdens the Government would face in providing greater process."

Provisional Quarantine.
The function involved is the administrative confinement—"provisional quarantine"[11]—of international and domestic airline passengers for three business days with no hearing of any kind, keeping in mind that being quarantined on a Friday could result in five days' confinement, or six days before a three-day weekend. Regardless of the government's interest in protecting public health, three days without the opportunity to challenge one's detention is a long time; five or six days is unacceptable, especially since an unknown number of people will be quarantined based on false positives screenings. In addition, the regulations are silent as to whether a passenger put into provisional quarantine is effectively incommunicado for the prescribed period, or may contact family, friends, their own doctor, and possibly an attorney.

Another reason we consider it necessary for individuals in provisional quarantine to have access to the full panoply of due process rights, including a hearing, is that there is always the potential for abuse of the CDC's authority to detain someone the government doesn't like using the possibility of communicable diseases as a pretext. We repeat that three days without recourse is a long time.

The stated three-day duration of provisional quarantine also seems arbitrary and confusing in view of information about disease incubation periods (see the table on page 71904). For example, if the incubation period for infectious TB is 4-6 weeks, and for Ebola is 2-21 days, how useful is a 3-day provisional quarantine to decide if someone is infected with either disease? Is the CDC being disingenuous in setting a 3-day period? In the case of a suspected disease with a longer

[10] *Ibid.*
[11] 42 CFR 70.14 and 71.17.

incubation period, would the provisional quarantine automatically be extended until someone either tested positive or reached the end of the prescribed incubation period still testing negative? If the provisional quarantine period is in reality as flexible as the incubation period for a given disease, do the due process limitations in the proposed regulations—no right to a hearing during the provisional quarantine—apply to a considerably extended provisional quarantine?

Full Quarantine.
Under the proposed regulations, only persons in actual quarantine, not provisional quarantine, may request a hearing (42 CFR Parts 70.16 to 71.20 and 71.19 to 71.23). The regulations, however, are confusing and it is difficult to understand what actual recourse quarantined passengers have.

Part 70.20 gives someone who has been placed in quarantine the right to an administrative hearing, but subpart (j) gives the CDC Director authority to "issue additional instructions and guidelines as the Director deems necessary governing the conduct of hearings." This would appear to give the Director, not the appointed hearing officer, ultimate authority over the hearings and the ability to control their outcome. It also has the potential to be a serious constraint on due process

It is also unclear whether the Director's decision is appealable. Part 70.20(k) states that a "quarantine order shall be deemed final either when the Director has accepted or rejected the hearing officer's written recommendation or three business days after the request for a hearing, whichever comes first." It appears not to be appealable, in view of the fact that Part 70.31 specifically allows written appeals only for Parts 70.6 and 70.7 (application for travel permit denied), 70.11 (order of destruction of animals or property), and Part 70.12 (detention of carrier). There is no mention of an appeal of the Director's decision (Part 70.20(k)). Also, Part 70.20 does not forthrightly say that the Director's decision on a quarantine order is "final agency action," but it should do so, as Part 70.31 does: the Director's resolution of the appeal "shall constitute final agency action." This presumably means the Director's decision is subject to judicial review under the Administrative Procedures Act, unless the quarantine orders are exempt from the APA.

Whether quarantine orders are in fact exempt from the APA is a matter of confusion. As noted above, Part 70.31 specifies the orders that are eligible for a written appeal; quarantine orders are not included. Part 70.20 doesn't clearly say that the Director's decision on a quarantine order is a final agency action. The introductory section of the Federal Register notice says, "An opportunity to request an administrative hearing for purposes of reviewing the quarantine order is provided for under these regulations [but it doesn't seem to be]. The person or group may also seek judicial review of the quarantine order through a petition for writ of habeas corpus pursuant to 28 U.S.C. 2241."[12] Also, "Under 28 USC 2241,

[12] Page 71904.

an opportunity for judicial review of the agency's decision exists via the filing of a petition for a writ of habeas corpus."[13]

The CDC should resolve this confusion by making clear in its final regulations that the Director's decision on a quarantine order is final agency action and that it is subject to judicial review under the APA, or alternatively by writ of habeas corpus.

Notice.
The regulations for provisional quarantine orders (42 CFR Parts 70.15 and 71.18) call for either personal service of a written order containing information specific to the individual served, or, alternatively, in the Director of CDC's discretion, posting or publication. We believe that anything short of personal notice is inadequate for due process in this situation. There is too much required information in the notice, on which later appeals of quarantine may depend to allow for anything other than personal notice. Proper notice must state all of the following:

> (1) A statement regarding the basis for the Director's reasonable belief that the person or group of persons is in the qualifying stage of a quarantinable disease based on information available to the Director at the time, such as travel history, clinical manifestations, or any other evidence of infection or exposure;
> (2) A statement setting forth the Director's reasonable belief that either:
> (i) The person or group of persons is moving or about to move from a State to another State; or
> (ii) A probable source of infection to persons who will be moving from a State to another State;
> (3) The suspected quarantinable disease;
> (4) A statement advising the person or group or persons that they may be under provisional quarantine for three business days and that at the end of such period they shall be released or, if determined by the Director, served with a quarantine order;
> (5) A statement advising the person or group of persons that they may be released earlier if the Director determines that provisional quarantine is no longer warranted;
> 6) The location of provisional quarantine.[14]

Also, considering the fact that many people ordered into provisional quarantine will not speak English, a sign posted in the health inspection area of airport customs stating that all arriving passengers are hereby ordered into provisional quarantine will be of little use, either to provide necessary information in the moment or as evidence in any future appeal. A personal, printed notice at least holds the possibility that it can eventually be translated.

[13] Page 71896.
[14] Page 71933.

7 Passenger Data

The CDC proposes to require airlines, cruise and other passenger ship lines and GDSs (global distribution systems, also known as computerized reservation systems or CRSs) to collect a vast amount of passenger information. (Passenger information, 42 CFR Parts 70.4 and 71.10). We have questions about the quantity of information the CDC wishes to have collected, as well as privacy and security practices for handling the information.

The Regulations Should Clearly State That Passengers Who Do Not Provide Contact Information Will Not Be Prevented from Traveling.
We note that neither Part 70.4 nor 71.10 specifically reflects a statement in the introductory section of the notice that "passengers who decline to provide contact information will not be prohibited from traveling."[15]

We suggest adding following express language to subpart (a) of Parts 70.4 and 71.10: "Airlines may not prohibit passengers who decline to provide contact information specified in paragraph (e) of this section from traveling." We also suggest explaining what consequences there are in terms of the regulations concerning screening and quarantine, if any, for passengers who decline to provide the requested personal information at the time they make a reservation. If the Director decrees that all passengers coming from a certain airport or seaport shall be screened on arrival in the U.S., will they be compelled to give the information detailed in Part 70.4 at that time? If so, the final regulations should include that requirement, whether a person may decline, and what the consequences of not providing the information are.

Required Passenger Information.
Part 70.4(e) of the proposed regulations asks for at least 18 individual elements of personal information. No airline or GDS currently collects all this information and there is no consistency in the information different companies collect at the time a reservation is made. Also, no installed system has the data fields to accommodate even the "basic" information the CDC wants to have collected, let alone the unknown number of additional data fields required for emergency contact information and names of traveling companions or group:

(1) Full name (first, last, middle initial, suffix);
(2) Emergency contact information;
(3) E-mail address;
(4) Current home address (street, apartment , city, state/province, postal code);
(5) Passport number or travel document number, including the issuing country or organization (in the case of foreign nationals only);
(6) Names of traveling companions or group;
(7) Flight information;
(8) Returning flight (date, airline number, and flight number);

[15] Page 71899.

(9) At least one of the following current phone numbers (in order of preference): mobile, home, pager, or work;
(f) In addition to data fields specified in paragraph (e) of this section, when necessary to prevent the introduction, transmission, or spread of communicable diseases, the Director through order may also require that airlines transmit additional information in the airline's possession.

The CDC Proposes to Collect Far More Information Than Necessary to Accomplish Its Purpose.
CDC's purpose in the sections of these rules that deal with data collection, storage and transfer is to be able to contact passengers at risk of infection with a communicable disease after they have dispersed from their travels. To return to Judge Kozinski's point, assuming that this represents a compelling need for the government to require private companies to collect personal information in excess of or different from what they would normally collect, store, and transfer it to the CDC on demand, the government's intrusion into individual privacy and the burden it places on private business should be strictly limited to fulfilling the exact need involved. The proposed regulations call for personal information far in excess of this need and also in excess of what it is reasonable for the government to know about people, such as the names of the individuals or group of individuals they are traveling with. This information is only indirectly necessary as a possible fallback to contact someone should other more direct means fail. Against such marginal utility, requiring information about whom one is traveling with represents a serious intrusion on First Amendment freedom of association and the Fifth Amendment right against self-incrimination (e.g., guilt by association with someone who may be on a watch list).

Furthermore, Part 70.4(f), authorizing the CDC director to require airlines to turn over whatever additional information they have in their possession—a kind of "wild-card" provision—is simply a fishing expedition. Again, it represents an unreasonable government demand for personal information and is also in excess of the minimum intrusion necessary to accomplish the regulations' stated goal of contacting someone that the CDC should be aiming for in establishing this tracking program.

We believe that two pieces of information would be sufficient to accomplish this goal: 1) name; and 2) telephone number. Full name (first, last, middle initial, suffix) is not necessary, because it is the ability to reach the person that is essential, not what his middle initial is. To facilitate contact, whatever name elements a reservation system currently collects would serve the purpose. As for being able to reach a person, one means of contact is sufficient, with alternate choices of which one is the most direct and immediate, depending on circumstances:

- For a domestic traveler with a domestic destination, the first choice would be cell phone number, followed by pager, then home phone number.

- For a U.S. traveler with a foreign destination, cell phone number if the phone has international capability, then emergency contact information.
- U.S. traveler returning to the U.S. from abroad, cell phone number, followed by pager, then home phone number.
- Foreign traveler entering the U.S., cell phone number if the phone has international capability, or emergency contact phone number if it does not.
- Alternatively, name plus emergency contact number might work for all contact scenarios and might also be the most efficient adaptation for reservations databases to make.

With the example of the TSA in mind, the CDC should consider extremely carefully and thoroughly test which data elements most reliably result in the ability to contact someone before deciding what information to require and instructing reservation-making entities what to collect. Because the information currently collected by reservation systems varies greatly, test data that includes all or even most of the elements suggested above is unlikely to be available from the companies involved. For that reason, CDC tests will likely have to be conducted without actual passenger data. One way to acquire the necessary data to test all variables would be, after publishing an appropriate System of Records Notice for temporary collection of data, to set up sample reservations web sites that collect all the proposed fields and see what the minimum information is that results in contact. Volunteers for testing could be solicited through media announcements or drawn from willing HHS employees.

Information Collection and Security Practices.
It is unclear from the Federal Register notice how CDC proposes to safeguard the personal information it wants carriers to collect, retain and transfer. The regulations seem to skirt around issues of collection and retention without stating a clear policy. Does CDC envision getting this data through DHS/APIS/Secure Flight (see the table on page 71899, with the headings "Data elements required by CDC NPRM," "Currently collected by airlines," and "Required by DHS/APIS for international flights")?

Parts 70.4(g) and 71.10(h) of the proposed regulations represent an attempt to impose fair information practices by restricting those collecting passengers' personal information to using it only for the purposes for which it was collected. The question is, for whose purposes was it collected? If only the minimum data elements the commenters suggest are required (name + most reliable phone number), that may be the same information airlines, shiplines and GDSs already collect and use according to their own purposes, limited (or not) by their own privacy policies.[16] If CDC requires information in excess of what companies currently collect, it is still being collected as part of the reservation process, so what is to prevent companies from using it within the restrictions of their own

[16] The utility of corporate privacy policies in protecting personal information is probably illusory anyway, in view of multiple airlines' transfer of around 12 million passenger records to TSA in violation of their privacy policies.

privacy policies? We believe the question of who controls the data collected by carriers and reservation services for CDC will inevitably intrude. One solution to the problem is to collect CDC information in an entirely separate database, impose strict security and access control, with timed destruction of all data and backups built into the system.

Is the CDC also restricted to using the information only for the purpose for which it's collected, i.e., to contact travelers in the event that they may have been exposed to a communicable disease? The Privacy Act has proven to be a somewhat theoretical protection for personal information because of the "routine use" exemption. Once the CDC has possession of whatever amount of personal information is settled on as the necessary minimum for contact, will it find other routine uses for the data, such as research (the data gives the agency the ability to contact individuals to participate in studies) or statistical analysis (possibly in the aggregate, with personally identifying information removed). Will it be available for routine use by other government agencies? It is already understood that it will be available for any national security purposes, such as an investigation to find the intentional carrier of a bioengineered epidemic disease (the suicide virus bomber).

Parts 70.4(h) and 71.10(i) require that notice be given to passengers of the purposes of the information collection at the time they make their reservations or travel arrangements. The means of doing this is left up to the collecting entity. Given the extent to which private companies are known to obscure the purposes for which they intend to use personal information they collect, we are skeptical that passengers will be meaningfully informed. How informative a notice companies provide becomes all the more problematic in view of the fact that people might reconsider their travel plans if they are notified at the time they make a reservation that they must give information that will enable the CDC to contact them personally in the event that they may have been exposed to a dangerous communicable disease.

Information Handling and Security.
Parts 70.5 and 71.11 (Written plan for passenger information and designation of an airline or shipline agent) deal with information handling practices that will enable the CDC to implement its passenger contact plan. Subsection (a) of both parts gives all interstate and international airlines and shiplines six months from the date of the final notice of these regulations to come up with a written plan for handling all the information CDC requests. Based in part on TSA's almost 4-year experience trying to develop a system for collection and transfer of certain passenger information in cooperation with the airlines, we believe that this is not a realistic timeframe. However, the companies that must produce a written plan are better qualified to comment on how long it will take them to arrive at a viable one.

Security Standards. The commenters are extremely concerned with the security standard the regulations call for:

> Part 70.5(b)(1) Policies and procedures for the transmission of data in an electronic format available to both the airline and the Director [of CDC] using *industry standards* for data encoding, transmission, and security. (emphasis added)

The news about industry standards for data security in 2005 is not a good recommendation for industry standards. Privacy Rights Clearinghouse, the San Diego-based consumer advocacy group, has assembled a chronology of data breaches since February 2005. That was when the requirements of California's security breach notice law[17] compelled broker Choicepoint to disclose that it had sold the personal information of 145,000 people to thieves who set up fake accounts to buy it—because it was forced to notify the victims. As of January 12, 2006, Privacy Rights Clearinghouse has logged security breaches compromising the personal information of more than 52 million people, variously caused by hackers, dishonest insiders, lost or stolen equipment or data on portable media, and other deliberate or inadvertent means. (See "A Chronology of Data Breaches Reported Since the ChoicePoint Incident," http://www.privacyrights.org/ar/ChronDataBreaches.htm) Also, in the aftermath of the Choicepoint data security scandal, at least 23 states have passed their own breach notices laws.[18]

It is unfortunate that regardless of industry standards, there will always be dishonest insiders and inadvertent or inattentive slip-ups that lead to exposure of personal information, such as thoughtlessly constructed web sites or laptops left in cars. That is no reason, however, for not requiring airlines and shiplines to use the best available security standards for collecting passenger information required by the CDC, for storing it for 60 days from the completion of travel, and for transferring it when it's requested.

What Happens to the Data After the Mandatory Retention Period?
Airlines currently delete passenger manifests within a few days of completion of a flight; it is not known what the practices of cruise and passenger shiplines are with regard to manifests. If, however, the CDC requires airlines to retain the passenger data it is ordering them to collect for 60 days after the completion of travel, once they have made the changes necessary to their reservation and information storage systems to do this, what is to prevent them from keeping the data indefinitely and using it, perhaps for marketing purposes? In spite of the provision restricting use of the data to the purpose for which it is collected (42 CFR Parts 70.4(g) and 71.10(h)), it is the airlines that control the data. Furthermore, it is the airlines that can claim legal ownership of information voluntarily turned over to them by passengers making reservations. As a practical matter, unless the regulations require the information specifically requested by

[17] California Civil Code Sec. 1798.80-1798.82. Requires notice to consumers of a breach in the security, confidentiality, or integrity of unencrypted personal information held by a business or government agency.
[18] For a list of state security breach notice laws see http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf

CDC to be kept separately from regular passenger reservation data, it will not be separable from the standard data, since it includes the most basic data field and the one common to all reservation systems—the passenger's name.

Proposed Additions to the Final Rules for Information Handling to Address the Issues Raised Above.
We recommend the following improvements to regulations for handling of passenger data by carriers and the CDC:

- The carriers and GDSs should maintain data they are collecting at the request of CDC, including the fields that overlaps what their own reservation systems collect, in a separate database protected by meaningful access controls (such as passwords), very restricted access (there is no reason why any airline should consult this database), and a secure audit trail.
- Part 70.4(b), which says that the data is to be kept for 60 days, should be amended to add: "Airlines shall also ensure that such information is automatically erased after 60 days, and file with the Director a detailed specification of the means by which such automatic erasure shall be achieved." A definition of "erasure" should also be added to Part 70.1: "erasure means to ensure that the data is not recoverable; erasure is not complete unless all backups are also erased."
- Part 70.4 should expressly state that the sole purpose of this data collection is "to prevent the introduction, transmission, or spread of communicable diseases."
- Part 70.4(g) should have an additional sentence to the effect that "Providing access to or disclosing or disseminating such information for any other purpose is strictly prohibited."
- An audit mechanism should be established to ensure that Part 70.4(g)—"Information collected solely in order to comply with this regulation may only be used for the purposes for which it is collected" —is enforceable. We suggest that CDC should periodically and randomly review all audit logs relating to the passenger information database to check for improper access as well as data destruction after 60 days.

To rectify what appears to be a wholesale omission of regulations concerning CDC's own handling of the data, we recommend at a minimum that the discussion in the introductory section of the Federal Register notice at pp. 71899-71900 be expressly reflected in the regulations themselves. That is, regulations should be added to make practices concerning collection for authorized purposes, security of paper and electronic records and destruction of data legally binding. The proposed regulations do not this and the default is the existing rules, which we believe are inadequate.

Data Collection and the European Union Data Protection Directive.
It should be noted that litigation over the TSA's request (coupled with the threat to deny U.S. landing rights) to European airlines to turn over their passenger

name records (PNRs) is still ongoing in the European Union Court of Justice. The case was brought by members of the European Parliament who disagreed with the decision of the European Commission to bypass the Data Protection Directive and transfer Europeans' PNRs to the TSA, because they believed TSA would not "adequately protect" the data up to the Directive's standards. As a practical matter, it seems unlikely that the Data Protection Directive will be allowed to block transfer of passenger data requested for security screening purposes. There is a possibility, though, that the Court will adopt its Advocate General's opinion "that international transfers of personal data for law enforcement purposes are outside *any* authority of the EU—and thus, implicitly, that they could be authorized, if at all, only by *national* action by individual EU member governments, according to their various national procedures."[19] (emphasis in original) This would require CDC to reach a separate agreement with each of the countries in which the various European airlines, shiplines and reservation services are based.

8 Mission Creep

In a pandemic emergency or under the perceived threat of a bioengineered virus, there is no limit to the information collecting and tracking requirements, as well as the number of people detained in provisional quarantine without even minimal due process, the need to protect the public health could impose on the public. As noted, the "Director's authority to investigate suspected cases and potential spread of communicable disease among foreign and interstate travelers is thus not limited to those known or suspected of having a quarantinable disease."[20] This is an extremely, and in our view unacceptably, broad mandate to take actions that impinge on the exercise of constitutional rights. The ability to impose quarantine even on those not "known or suspected of having a quarantinable disease" is tantamount to a police power, and it could easily be abused.

In these regulations the CDC already claims authority to collect contact information for people traveling by air between states or within a state. Under what threat scenario would information collection and individual tracking be extended to trains and interstate buses, to private tour buses (such as the innumerable casino buses), and inter- and intra-state ferries? If mass transit fares become nationally smart-card based, will municipal transportation agencies be required to collect and maintain personally identifiable records of commuters that include all the data fields the CDC requires?

We believe that the CDC's intention is to fulfill its responsibility as the public health watchdog to be well-prepared to act quickly and effectively in the event of an infectious disease emergency. We are concerned, however, that reasons will be

[19] "EU Court advisory opinion against USA access to airline reservation data," Edward Hasbrouck, The Practical Nomad (blog), November 27, 2005, http://hasbrouck.org/blog/archives/000927.html.
[20] Page 71899.

found to collect information on citizens engaged in perfectly mundane local travel, such as commuting in subways or buses, in order to be able to contact and notify them that they may have been exposed to a communicable disease or intentionally released bioagent.

9 Conclusions

There is a clear need for the CDC to be able to contact travelers in the event of exposure to a communicable disease. The regulations CDC proposes with regard to screening and quarantine procedures, however, raise serious constitutional issues of rights under the First, Fourth and Fourteenth Amendments. Balancing government authority against citizens' rights is essential to the legislation and regulation process. Regulations, especially, require very careful tailoring when they will impact the right to travel, freedom of movement and freedom of association, as well as protections against search and seizure, even taking administrative exceptions into account. And basic due process requires that detention in quarantine for any period of time, along with the ability to appeal a quarantine order, be accounted for.

Based on the experiences of the TSA to date in collecting and handling passenger data. CDC must have clear policies in place for its own collection and handling of personal information.

Respectfully submitted,

Linda Ackerman
Staff Counsel
Privacy Activism

Beth Givens
Executive Director
Privacy Rights Clearinghouse

Mike Stollenwerk
Executive Director
Fairfax County Privacy Council

APPENDIX A

New York Times
Military Hardware Is Adapted to Fight SARS
By WAYNE ARNOLD

SINGAPORE, May 11 Authorities in Singapore have adapted devices originally developed for a military purpose seeing enemies in the dark to help combat the spread of SARS.

The new version of the device, called an infrared fever sensing system, detects passengers' body temperatures, spotting people with a fever one of the symptoms of SARS without having to touch them or even make them stop walking. The system, which is said to be is easy to use, was developed in a week.

Now, instead of having to pass a phalanx of inquisitive nurses, passengersarriving in Singapore simply walk past a camera. Those who appear to have afever are taken aside for a closer look by a technician.

The device has become so coveted by immigration authorities and other officials around the world who are hoping to spot infectious people that the creators of the system are planning to begin commercial production, in partnership with the Solectron Corporation of Milpitas, Calif.

Development of the system began with a telephone call in early April from the Ministry of Health to Singapore's Defense Science and Technology Agency, asking for a more efficient way of screening incoming passengers for fever.

"The problem wasn't new to us, because we were watching the TV," said Tan Yang How, the agency's division manager for sensor systems. Aside from being slow and intrusive, the use of nurses to screen all incoming passengers was a waste of skilled medical staff. "Nurses are needed back in hospital," Mr. Tan said. The agency in turn asked the Singapore Armed Forces to lend 50 of its thermal imaging scanners, used to help weapons systems locate targets that cannot be seen otherwise.

Together with Singapore Technologies Electronics, the manufacturer of the scanners, more than 30 engineers at the agency worked to modify the devices for the new purpose. Two flat-panel displays were added, along with an adapter to allow it to be plugged into an ordinary electrical socket. Engineers then took software originally designed to interpret thermal data to find cracks in rail lines and adapted it to search for hot people.

The finished product, which rolled into the airport a week later, is housed in a stainless steel trolley rather like a hot-dog stand. In place of an umbrella, the trolley has a camera covered in a black cowl, with only the lens protruding. One display screen sits on top of the trolley, and another is on a stand facing oncoming travelers.

The camera "sees" the warmth of objects relative to the ambient temperature, and translates that information into a video image of people walking by. The customized software is set to display anything cooler than 93.2 degrees as black. Normal exposed skin in the mid-90's registers as lime green, brightening to yellow as it gets warmer. Anything at 99.5 degrees or above, like a feverish forehead, glows bright red in the image.

The system is remarkably sensitive, able to discern temperatures to within one-half a degree at a range of 15 feet. It can see warm bodies much farther away, though less precisely.

Of course, not every fever is a sign of SARS, and a fever is not the only reason a person might redden on the screen, according to Ace Cheong, an operator of one of the devices.

A sunburn, a few drinks of alcohol or just some brisk exercise might raise skin temperature enough to earn a trip to the special cubicle nearby for an encounter with an oral thermometer, Mr. Cheong said. He said that having eaten mutton or smoked a cigarette recently can also produce a red response.

Singapore has 25 of the devices on trolleys deployed at Changi Airport, at ferry terminals and at the two causeways linking the city-state to neighboring Malaysia. It has lent several more to officials in Hong Kong and Canada.

But Singapore Technologies Electronics has bigger plans, according to Tay Hun Kiat, who heads the company's operations in Asia and the Pacific.

With orders for 110 more units in hand, the company has contracted with Solectron to begin producing commercial versions in a factory that now makes servers and circuit boards for Hewlett-Packard and I.B.M. The first off the line will sell for about $50,000 apiece.